SYS.4.3.A8 Einsatz eines sicheren Betriebssystems für eingebettete Systeme (S) [Entwickelnde, Planende, Beschaffungsstelle]

Das eingesetzte Betriebssystem und die Konfiguration des eingebetteten Systems SOLLTEN für den vorgesehenen Betrieb geeignet sein. So SOLLTE das Betriebssystem für die vorgesehene Aufgabe über ausreichende Sicherheitsmechanismen verfügen. Die benötigten Dienste und Funktionen SOLLTEN aktiviert sein. Das Betriebssystem SOLLTE es unterstützen, ein Trusted Plattform Module (TPM) zu nutzen.

SYS.4.3.A9 Einsatz kryptografischer Prozessoren bzw. Koprozessoren bei eingebetteten Systemen (S) [Entwickelnde, Planende, Beschaffungsstelle]

Wird ein zusätzlicher Mikrocontroller für die kryptografischen Berechnungen verwendet, SOLLTE dessen Kommunikation mit dem System-Mikrocontroller ausreichend abgesichert sein. Für das eingebettete System SOLLTEN die nötigen Vertrauensanker realisiert werden. Auch SOLLTE eine Vertrauenskette (Chain of Trust) implementiert sein.

SYS.4.3.A10 Wiederherstellung von eingebetteten Systemen (S)

Eingebettete Systeme SOLLTEN über Rollback-Fähigkeiten verfügen.

SYS.4.3.A11 Sichere Aussonderung eines eingebetteten Systems (S)

Bevor eingebettete Systeme ausgesondert werden, SOLLTEN sämtliche Daten auf dem System sicher gelöscht werden. Ist dies nicht möglich, SOLLTE das System vernichtet werden. Die Löschung oder Vernichtung SOLLTE dokumentiert werden.

3.3. Anforderungen bei erhöhtem Schutzbedarf

Im Folgenden sind für diesen Baustein exemplarische Vorschläge für Anforderungen aufgeführt, die über dasjenige Schutzniveau hinausgehen, das dem Stand der Technik entspricht. Die Vorschläge SOLLTEN bei erhöhtem Schutzbedarf in Betracht gezogen werden. Die konkrete Festlegung erfolgt im Rahmen einer individuellen Risikoanalyse.

SYS.4.3.A12 Auswahl einer vertrauenswürdigen Lieferungs- und Logistikkette sowie qualifizierte herstellende Institutionen für eingebettete Systeme (H) [Beschaffungsstelle]

Es SOLLTEN in der Logistikkette wirksame Kontrollen durchgeführt werden, sodass sichergestellt ist,

- dass eingebettete Systeme keine manipulierten, gefälschten oder getauschten Komponenten enthalten,
- die Systeme der Spezifikation entsprechen und keine verdeckten Funktionen bei der Herstellung implementiert wurden sowie
- Unbefugte nicht an vertrauliche Informationen über das eingebettete System gelangen können.

Die beteiligten Unternehmen SOLLTEN nachweisbar qualifiziert sein.

SYS.4.3.A13 Einsatz eines zertifizierten Betriebssystems (H) [Entwickelnde, Planende, Beschaffungsstelle]

Das Betriebssystem SOLLTE nach einem anerkannten Standard auf einer angemessenen Stufe evaluiert sein.

SYS.4.3.A14 Abgesicherter und authentisierter Bootprozess bei eingebetteten Systemen (H) [Entwickelnde, Planende, Beschaffungsstelle]

Der Bootprozess eines eingebetteten Systems SOLLTE abgesichert sein, indem der Bootloader die Integrität des Betriebssystems überprüft und es nur dann lädt, wenn es als korrekt eingestuft wurde. Umgekehrt SOLLTE auch das Betriebssystem die Integrität des Bootloaders prüfen.

Es SOLLTE ein mehrstufiges Boot-Konzept mit kryptografisch sicherer Überprüfung der Einzelschritte realisiert werden. Sichere Hardware-Vertrauensanker SOLLTEN verwendet werden. Bei einem ARM-basierten eingebetteten System SOLLTE ARM Secure Boot genutzt werden. Bei einem Unified Extensible Firmware Interface (UEFI) SOLLTE Secure Boot genutzt werden.

SYS.4.3.A15 Speicherschutz bei eingebetteten Systemen (H) [Entwickelnde, Planende, Beschaffungsstelle]

Bereits beim Entwurf eingebetteter Systeme SOLLTEN Speicherschutzmechanismen berücksichtigt werden. Die Art des Speicherschutzes sowie Anzahl und Größe der Schutzräume SOLLTEN für den Einsatzzweck angemessen sein.

SYS.4.3.A16 Tamper-Schutz bei eingebetteten Systemen (H) [Planende]

Für eingebettete Systeme SOLLTE ein Tamper-Schutz-Konzept entwickelt werden. Es SOLLTEN angemessene Mechanismen etabliert werden, die Tamper-Angriffe erkennen, aufzeichnen und verhindern. Schließlich SOLLTEN angemessene Vorgaben etabliert werden, wie auf einen Tamper-Angriff zu reagieren ist.

SYS.4.3.A17 Automatische Überwachung der Baugruppenfunktion (H) [Planende, Beschaffungsstelle]

Sämtliche Baugruppen eines eingebetteten Systems mit erhöhten Anforderungen an die Verfügbarkeit und Integrität SOLLTEN integrierte Selbsttesteinrichtungen (Built-in Self-Test, BIST) besitzen. Tests SOLLTEN während des Einschaltvorgangs sowie in angemessenen zeitlichen Intervallen während des Betriebs die Integrität des Systems prüfen. Soweit möglich, SOLLTEN die Selbsttestfunktionen auch Sicherheitsfunktionen und Sicherheitseigenschaften der Baugruppe überprüfen.

Regelmäßig SOLLTE die Integrität der Speicher und I/O-Komponenten im Rahmen des BIST geprüft werden. Bestehende BIST-Funktionen SOLLTEN, falls möglich, um die erforderlichen Funktionen ergänzt werden.

SYS.4.3.A18 Widerstandsfähigkeit eingebetteter Systeme gegen Seitenkanalangriffe (H) [Entwickelnde, Beschaffungsstelle]

Es SOLLTEN angemessene Vorkehrungen gegen nicht-invasive und (semi-)invasive Seitenkanalangriffe getroffen werden.

4. Weiterführende Informationen

4.1. Wissenswertes

Das BSI gibt in seinem Dokument „ICS-Security-Kompendium – Testempfehlungen und Anforderungen für Herstellende von Komponenten“ Hilfestellungen für den Test der ICS-Komponenten und stellt Maßnahmen vor, um Schwachstellen zu vermeiden und zu erkennen.

Bundesamt
für Sicherheit in der
Informationstechnik

SYS.4.4 Allgemeines IoT-Gerät

1. Beschreibung

1.1. Einleitung

Geräte mit Funktionen aus dem Bereich Internet of Things (IoT) sind, im Gegensatz zu klassischen Endgeräten, vernetzte Geräte oder Gegenstände, die zusätzliche „smarte" Funktionen besitzen. IoT-Geräte werden in der Regel drahtlos an Datennetze angeschlossen. Die meisten Geräte können auf Informationen im Internet zugreifen und darüber erreicht werden. Hierdurch können sie Auswirkungen auf die Informationssicherheit des gesamten Informationsverbunds haben.

IoT-Geräte, wie Smartwatches oder andere Wearables, können in Institutionen gelangen, indem sie durch Mitarbeitende oder Externe am Körper getragen werden. In vielen Institutionen werden aber auch IoT-Geräte beschafft und betrieben, darunter etwa Brand-, Gas- und andere Warnmelder, Kaffeemaschinen oder Elemente der Gebäudesteuerung wie Kameras und HVAC (Heating, Ventilation and Air Conditioning).

Generell kann zwischen direkt adressierbaren IoT-Geräten und IoT-Geräten, die eine zentrale Steuereinheit voraussetzen, unterschieden werden. Direkt adressierbare Geräte werden in der Regel mit einer eigenen IP-Adresse an das LAN angeschlossen oder haben einen eigenen direkten Netzanschluss, z. B. mittels Mobilfunk, und können autark agieren oder durch eine zentrale Steuereinheit verwaltet werden. Daneben gibt es IoT-Geräte, die ausschließlich direkt mit Steuereinheiten kommunizieren, z. B. über Funknetze wie Bluetooth oder ZigBee, und somit nicht direkt an bestehende Datennetze angeschlossen werden.

1.2. Zielsetzung

Ziel dieses Bausteins ist es, IoT-Geräte so abzusichern, dass über diese weder die Informationssicherheit der eigenen Institution noch die von Außenstehenden beeinträchtigt wird. Daher sollte sowohl ein unautorisierter Datenabfluss als auch die Manipulation der Geräte verhindert werden, speziell mit Blick auf Angriffe durch Dritte.

1.3. Abgrenzung und Modellierung

Der Baustein SYS.4.4 *Allgemeines IoT-Gerät* ist auf jedes Gerät mit Funktionalitäten aus dem Bereich Internet of Things (IoT) anzuwenden.

Dieser Baustein beschäftigt sich allgemein mit IoT-Geräten und soll für ein großes Spektrum unterschiedlicher IoT-Geräte anwendbar sein. Auf dedizierte Sicherheitseigenschaften, etwa von Bedien- und Anzeigesystemen oder spezifischen Hard- und Software-Architekturen, wird nicht näher eingegangen.

Je nach Ausprägung der IoT-Geräte sind die Übergänge zu industriellen Steuerungssystemen (ICS-Systemen) oder eingebetteten Systemen fließend. Anforderungen an Geräte, die im Bereich Produktion und Fertigung eingesetzt werden, sind in den Bausteinen der Schicht IND *Industrielle IT* zu finden.

Eingebettete Systeme hingegen sind informationsverarbeitende Systeme, die in ein größeres System oder Produkt integriert sind, dort Steuerungs-, Regelungs- und Datenverarbeitungsaufgaben übernehmen und dabei oft nicht direkt von den Benutzenden wahrgenommen werden. Für diese Systeme ist der Baustein SYS.4.3 *Eingebettete Systeme* umzusetzen.

Anforderungen an die häufig im Zusammenhang mit IoT-Geräten eingesetzten Funkstrecken befinden sich in den Bausteinen der Schicht NET.2 *Funknetze*.

Die im betrachteten Informationsverbund eingesetzten IoT-Geräte sind im Identitäts- und Berechtigungsmanagement zu berücksichtigen. Hierfür ist der Baustein ORP.4 *Identitäts- und Berechtigungsmanagement* umzusetzen.

2. Gefährdungslage

Da IT-Grundschutz-Bausteine nicht auf individuelle Informationsverbünde eingehen können, werden zur Darstellung der Gefährdungslage typische Szenarien zugrunde gelegt. Die folgenden spezifischen Bedrohungen und Schwachstellen sind für den Baustein SYS.4.4 *Allgemeines IoT-Gerät* von besonderer Bedeutung.

2.1. Ausspähung über IoT-Geräte

Bei der Entwicklung von IoT-Geräten wird der Aspekt der Informationssicherheit typischerweise nicht oder nur nachrangig beachtet. Das sorgte in der Vergangenheit dafür, dass IoT-Geräte immer wieder dazu missbraucht wurden, um Informationen über die Benutzenden oder den Einsatzbereich zu sammeln. So sind immer wieder Vorfälle mit vernetzten bzw. IP-basierten Überwachungskameras eingetreten:

- 2021 wurden Überwachungskameras durch erneute Registrierung der Kamera-ID gehackt. Es konnte so die Steuerung übernommen werden.
- 2022 wurden Videostreams von Babymonitoren durch eine fehlende Authentisierung bei einem Angriff auf andere Server umgeleitet. Aufgrund der fehlenden Authentisierung war es sogar möglich die Steuerung zu übernehmen.

Ende September 2016 wurde bekannt, dass einige Modelle von Überwachungskameras und Raumsensoren mit Hintertüren ausgestattet sind, die Spionage ermöglichen. Dies betraf insbesondere Überwachungskameras, die in Rechenzentren und Serverräumen eingesetzt wurden. Die Hintertüren ermöglichten offenbar, dass auf die Bild- und Videodaten der Kameras zugegriffen werden konnte und dass diese Daten auf Server im Internet kopiert werden konnten. Auf diese Weise konnten z. B. Kennwörter von Benutzenden oder Administrierenden kompromittiert werden oder Gerätekonfigurationen, Infrastrukturdetails und sonstige vertrauliche Informationen Dritten zugänglich werden. Dies erleichterte weitergehende Angriffe, indem die Gewohnheiten der Mitarbeitenden ausgenutzt wurden.

2.2. Verwendung von UPnP

In LANs integrierte IoT-Geräte bauen oftmals selbstständig eine Verbindung zum Internet auf, indem sie Router im Netz per UPnP (Universal Plug and Play) so konfigurieren, dass eine Portweiterleitung entsteht. Die Geräte können dann nicht nur ins lokale Netz kommunizieren, sondern sind auch außerhalb des LANs sicht- und erreichbar. Wenn dann eine Schwachstelle im IoT-Gerät durch einen Angreifer ausgenutzt wird, könnte dieses Gerät Teil eines Botnetzes werden. Außerdem könnte weitere Schadsoftware in den Informationsverbund eingeschleust werden. Diese Sicherheitslücke kann zu einem späteren Zeitpunkt auch für weitere missbräuchliche Aktivitäten ausgenutzt werden.

2.3. Übernahme in ein Botnetz

Wenn IoT-Geräte nicht regelmäßig gepatcht werden, bleiben bekannte Schwachstellen offen und können für umfangreiche Angriffe ausgenutzt werden. Ein Ziel eines Angriffs könnte sein, die IoT-Geräte in ein Botnetz zu integrieren. In diesem Fall könnten sie beispielsweise dazu missbraucht werden, um DDoS-Angriffe (Distributed Denial of Service) auszuführen und die Verfügbarkeit von Diensten einzuschränken.

Häufig werden dazu Botnetze benutzt, die zu großen Teilen aus IoT-Geräten bestehen. Mit der Schadsoftware „Mirai“, die es bereits seit 2016 gibt, werden beispielsweise Webcams, Kameras, digitale Videorecorder, Router und Drucker in ein Botnetz integriert. Sie scannen dann selbstständig das Internet nach weiteren Geräten, um sie mit Schadsoftware zu infizieren und dem Botnetz hinzuzufügen. Zusätzlich gibt es auch weitere Varianten einer solchen Schadsoftware wie „Mozi“ oder „BotenaGo“, die 2019 und 2021 eine ähnliche Vorgehensweise anwendeten.

3. Anforderungen

Im Folgenden sind die spezifischen Anforderungen des Bausteins SYS.4.4 *Allgemeines IoT-Gerät* aufgeführt. Der oder die Informationssicherheitsbeauftragte (ISB) ist dafür zuständig, dass alle Anforderungen gemäß dem festgelegten Sicherheitskonzept erfüllt und überprüft werden. Bei strategischen Entscheidungen ist der oder die ISB stets einzubeziehen.

Im IT-Grundschutz-Kompendium sind darüber hinaus weitere Rollen definiert. Sie sollten besetzt werden, insofern dies sinnvoll und angemessen ist.

Zuständigkeiten	Rolle
Grundsätzlich zuständig	IT-Betrieb
Weitere Zuständigkeiten	Beschaffungsstelle, Haustechnik

Genau eine Rolle sollte *Grundsätzlich zuständig* sein. Darüber hinaus kann es noch *Weitere Zuständigkeiten* geben. Falls eine dieser weiteren Rollen für die Erfüllung einer Anforderung vorrangig zuständig ist, dann wird diese Rolle hinter der Überschrift der Anforderung in eckigen Klammern aufgeführt. Die Verwendung des Singulars oder Plurals sagt nichts darüber aus, wie viele Personen diese Rollen ausfüllen sollen.

3.1. Basis-Anforderung

Die folgenden Anforderungen MÜSSEN für diesen Baustein vorrangig erfüllt werden.

SYS.4.4.A1 Einsatzkriterien für IoT-Geräte (B)

IoT-Geräte MÜSSEN Update-Funktionen besitzen. Die herstellenden Unternehmen MÜSSEN einen Update-Prozess anbieten. Die Geräte MÜSSEN eine angemessene Authentisierung ermöglichen. Es DÜRFEN KEINE fest codierten oder herzuleitenden Zugangsdaten in den Geräten enthalten sein.

SYS.4.4.A2 Authentisierung (B)

Eine angemessene Authentisierung MUSS aktiviert sein. IoT-Gerate MÜSSEN in das Identitäts- und Berechtigungsmanagement der Institution integriert werden.

SYS.4.4.A3 ENTFALLEN (B)

Diese Anforderung ist entfallen.

SYS.4.4.A4 ENTFALLEN (B)

Diese Anforderung ist entfallen.

SYS.4.4.A5 Einschränkung des Netzzugriffs (B)

Der Netzzugriff von IoT-Geräten MUSS auf das erforderliche Minimum eingeschränkt werden. Dies SOLLTE regelmäßig kontrolliert werden. Dazu SOLLTEN folgende Punkte beachtet werden:

- Bei Verkehrskontrollen an Netzübergängen, z. B. durch Regelwerke auf Firewalls und Access Control Lists (ACLs) auf Routern, DÜRFEN NUR zuvor definierte ein- und ausgehende Verbindungen erlaubt werden.
- Die Routings auf IoT-Geräten und Sensoren, insbesondere die Unterdrückung von Default-Routen, SOLLTE restriktiv konfiguriert werden.
- Die IoT-Geräte und Sensoren SOLLTEN in einem eigenen Netzsegment betrieben werden, das ausschließlich mit dem Netzsegment für das Management kommunizieren darf.
- Virtual Private Networks (VPNs) zwischen den Netzen mit IoT-Geräten und Sensor-Netzen und den Management-Netzen SOLLTEN restriktiv konfiguriert werden.
- Die UPnP-Funktion MUSS an allen Routern deaktiviert sein.

3.2. Standard-Anforderungen

Gemeinsam mit den Basis-Anforderungen entsprechen die folgenden Anforderungen dem Stand der Technik für diesen Baustein. Sie SOLLTEN grundsätzlich erfüllt werden.

SYS.4.4.A6 Aufnahme von IoT-Geräten in die Sicherheitsrichtlinie der Institution (S)

In der allgemeinen Sicherheitsrichtlinie der Institution SOLLTEN die Anforderungen an IoT-Geräte konkretisiert werden. Die Richtlinie SOLLTE allen Personen, die IoT-Geräte beschaffen und betreiben, bekannt und Grundlage für

deren Arbeit sein. Die Umsetzung der in der Richtlinie geforderten Inhalte SOLLTE regelmäßig überprüft und die Ergebnisse sinnvoll dokumentiert werden.

SYS.4.4.A7 Planung des Einsatzes von IoT-Geräten (S)

Um einen sicheren Betrieb von IoT-Geräten zu gewährleisten, SOLLTE im Vorfeld geplant werden, wo und wie diese eingesetzt werden sollen. Die Planung SOLLTE dabei nicht nur Aspekte betreffen, die klassischerweise mit dem Begriff Informationssicherheit verknüpft werden, sondern auch normale, betriebliche Aspekte, die Anforderungen im Bereich der Sicherheit nach sich ziehen. Alle Entscheidungen, die in der Planungsphase getroffen wurden, SOLLTEN geeignet dokumentiert werden.

SYS.4.4.A8 Beschaffungskriterien für IoT-Geräte (S) [Beschaffungsstelle]

Der oder die ISB SOLLTE bei allen Beschaffungen von IoT-Geräten mit einbezogen werden. Bevor IoT-Geräte beschafft werden, SOLLTE festgelegt werden, welche Sicherheitsanforderungen diese erfüllen müssen. Bei der Beschaffung von IoT-Geräten SOLLTEN Aspekte der materiellen Sicherheit ebenso wie Anforderungen an die Sicherheitseigenschaften der Software ausreichend berücksichtigt werden. Eine Anforderungsliste SOLLTE erstellt werden, anhand derer die am Markt erhältlichen Produkte bewertet werden.

SYS.4.4.A9 Regelung des Einsatzes von IoT-Geräten (S)

Für jedes IoT-Gerät SOLLTE eine zuständige Person für dessen Betrieb benannt werden. Die Zuständigen SOLLTEN ausreichend über den Umgang mit dem IoT-Gerät informiert werden.

SYS.4.4.A10 Sichere Installation und Konfiguration von IoT-Geräten (S)

Es SOLLTE festgelegt werden, unter welchen Rahmenbedingungen IoT-Geräte installiert und konfiguriert werden. Die IoT-Geräte SOLLTEN nur von autorisierten Personen (Zuständige für IoT-Geräte, Administrierende oder vertraglich gebundene Dienstleistende) nach einem definierten Prozess installiert und konfiguriert werden. Alle Installations- und Konfigurationsschritte SOLLTEN so dokumentiert werden, dass die Installation und Konfiguration durch sachkundige Dritte anhand der Dokumentation nachvollzogen und wiederholt werden kann.

Die Grundeinstellungen von IoT-Geräten SOLLTEN überprüft und nötigenfalls entsprechend den Vorgaben der Sicherheitsrichtlinie angepasst werden. Falls möglich, SOLLTEN IoT-Geräte erst mit Datennetzen verbunden werden, nachdem die Installation und die Konfiguration abgeschlossen sind.

SYS.4.4.A11 Verwendung von verschlüsselter Datenübertragung (S)

IoT-Geräte SOLLTEN Daten nur verschlüsselt übertragen.

SYS.4.4.A12 ENTFALLEN (S)

Diese Anforderung ist entfallen.

SYS.4.4.A13 Deaktivierung und Deinstallation nicht benötigter Komponenten (S)

Nach der Installation SOLLTE überprüft werden, welche Protokolle, Anwendungen und weiteren Tools auf den IoT-Geräten installiert und aktiviert sind. Nicht benötigte Protokolle, Dienste, Anmeldekennungen und Schnittstellen SOLLTEN deaktiviert oder ganz deinstalliert werden. Die Verwendung von nicht benötigten Funkschnittstellen SOLLTE unterbunden werden.

Wenn dies nicht am Gerät selber möglich ist, SOLLTEN nicht benötigte Dienste über die Firewall eingeschränkt werden. Die getroffenen Entscheidungen SOLLTEN so dokumentiert werden, dass nachvollzogen werden kann, welche Konfiguration für die IoT-Geräte gewählt wurden.

SYS.4.4.A14 ENTFALLEN (S)

Diese Anforderung ist entfallen.

SYS.4.4.A15 Restriktive Rechtevergabe (S)

Die Zugriffsberechtigungen auf IoT-Geräte SOLLTEN möglichst restriktiv vergeben werden. Wenn dies über die IoT-Geräte selber nicht möglich ist, SOLLTE überlegt werden, dies netzseitig zu regeln.

SYS.4.4.A16 Beseitigung von Schadprogrammen auf IoT-Geräten (S)

Der IT-Betrieb SOLLTE sich regelmäßig informieren, ob sich die eingesetzten IoT-Geräte mit Schadprogrammen infizieren könnten und wie Infektionen beseitigt werden können. Schadprogramme SOLLTEN unverzüglich beseitigt werden. Kann die Ursache für die Infektion nicht behoben bzw. eine Neuinfektion nicht wirksam verhindert werden, SOLLTEN die betroffenen IoT-Geräte nicht mehr verwendet werden.

SYS.4.4.A17 Überwachung des Netzverkehrs von IoT-Geräten (S)

Es SOLLTE überwacht werden, ob die IoT-Geräte oder Sensor-Systeme nur mit IT-Systemen kommunizieren, die für den Betrieb der IoT-Geräte notwendig sind.

SYS.4.4.A18 Protokollierung sicherheitsrelevanter Ereignisse bei IoT-Geräten (S)

Sicherheitsrelevante Ereignisse SOLLTEN automatisch protokolliert werden. Falls dies durch die IoT-Geräte selber nicht möglich ist, SOLLTEN hierfür Router oder Protokollmechanismen anderer IT-Systeme genutzt werden. Die Protokolle SOLLTEN geeignet ausgewertet werden.

SYS.4.4.A19 Schutz der Administrationsschnittstellen (S)

Abhängig davon, ob IoT-Geräte lokal, direkt über das Netz oder über zentrale netzbasierte Tools administriert werden, SOLLTEN geeignete Sicherheitsvorkehrungen getroffen werden. Der Zugriff auf die Administrationsschnittstellen von IoT-Geräten SOLLTE wie folgt eingeschränkt werden:

- Netzbasierte Administrationsschnittstellen SOLLTEN auf berechtigte IT-Systeme bzw. Netzsegmente beschränkt werden.
- Es SOLLTEN bevorzugt lokale Administrationsschnittstellen am IoT-Gerät oder Administrationsschnittstellen über lokale Netze verwendet werden.

Die zur Administration verwendeten Methoden SOLLTEN in der Sicherheitsrichtlinie festgelegt werden. Die IoT-Geräte SOLLTEN entsprechend der Sicherheitsrichtlinie administriert werden.

SYS.4.4.A20 Geregelte Außerbetriebnahme von IoT-Geräten (S)

Es SOLLTE eine Übersicht darüber geben, welche Daten wo auf IoT-Geräten gespeichert sind. Es SOLLTE eine Checkliste erstellt werden, die bei der Außerbetriebnahme von IoT-Geräten abgearbeitet werden kann. Diese Checkliste SOLLTE mindestens Aspekte zur Datensicherung weiterhin benötigter Daten und dem anschließenden sicheren Löschen aller Daten umfassen.

3.3. Anforderungen bei erhöhtem Schutzbedarf

Im Folgenden sind für diesen Baustein exemplarische Vorschläge für Anforderungen aufgeführt, die über dasjenige Schutzniveau hinausgehen, das dem Stand der Technik entspricht. Die Vorschläge SOLLTEN bei erhöhtem Schutzbedarf in Betracht gezogen werden. Die konkrete Festlegung erfolgt im Rahmen einer individuellen Risikoanalyse.

SYS.4.4.A21 Einsatzumgebung und Stromversorgung (H) [Haustechnik]

Es SOLLTE geklärt werden, ob IoT-Geräte in der angedachten Einsatzumgebung betrieben werden dürfen (Schutzbedarf anderer IT-Systeme, Datenschutz). IoT-Geräte SOLLTEN in der Einsatzumgebung vor Diebstahl, Zerstörung und Manipulation geschützt werden.

Es SOLLTE geklärt sein, ob ein IoT-Gerät bestimmte Anforderungen an die physische Einsatzumgebung hat, wie z. B. Luftfeuchtigkeit, Temperatur oder Energieversorgung. Falls erforderlich, SOLLTEN dafür ergänzende Maßnahmen bei der Infrastruktur umgesetzt werden.

Wenn IoT-Geräte mit Batterien betrieben werden, SOLLTE der regelmäßige Funktionstest und Austausch der Batterien geregelt werden.

IoT-Geräte SOLLTEN entsprechend ihrer vorgesehenen Einsatzart und dem vorgesehenen Einsatzort vor Staub und Verschmutzungen geschützt werden.

SYS.4.4.A22 Systemüberwachung (H)

Die IoT-Geräte SOLLTEN in ein geeignetes Systemüberwachungs- bzw. Monitoringkonzept eingebunden werden. Der Systemzustand und die Funktionsfähigkeit der IoT-Geräte SOLLTEN laufend überwacht werden. Fehlerzustände sowie die Überschreitung definierter Grenzwerte SOLLTEN an das Betriebspersonal gemeldet werden. Es SOLLTE geprüft werden, ob die verwendeten Geräte die Anforderung an die Verfügbarkeit erfüllen. Alternativ SOLLTE geprüft werden, ob weitere Maßnahmen, wie das Einrichten eines Clusters oder die Beschaffung von Standby-Geräten, erforderlich sind.

SYS.4.4.A23 Auditierung von IoT-Geräten (H)

Alle eingesetzten IoT-Geräte SOLLTEN regelmäßig auditiert werden.

SYS.4.4.A24 Sichere Konfiguration und Nutzung eines eingebetteten Webservers (H)

In IoT-Geräten integrierte Webserver SOLLTEN möglichst restriktiv konfiguriert sein. Der Webserver SOLLTE, soweit möglich, NICHT unter einem privilegierten Konto betrieben werden.

4. Weiterführende Informationen

4.1. Wissenswertes

Im Dokument „Sicherheit von Geräten im Internet der Dinge“ gibt das BSI einen Überblick über die elementaren Best Practices zum sicheren Betrieb von IoT-Kameras zu geben.

Das Department of Homeland Security (DHS) hat im Dokument „Strategic Principles for securing the Internet of Things (IoT)“ strategische Grundsätze für die Sicherheit von IoT-Geräten veröffentlicht.

Das Open Web Application Security Project (OWASP) stellt auf seiner Webseite Hinweise zur Absicherung von IoT-Geräten zur Verfügung.

Der europäische Standard ETSI EN 303 645 „Cyber Security for Consumer Internet of Things: Baseline Requirements“ dient als Empfehlung für die sichere Entwicklung von IoT-Geräten (Security by Design). Hierzu gehören unter anderem sichere Authentisierungsmechanismen, ein angemessenes Updatemanagement und die Absicherung der Kommunikation. Er findet unter anderem auch beim IT-Sicherheitskennzeichen des BSI Anwendung in verschiedenen Produktkategorien des IoT.

Bundesamt
für Sicherheit in der
Informationstechnik

SYS.4.5 Wechseldatenträger

1. Beschreibung

1.1. Einleitung

Wechseldatenträger werden oft eingesetzt, um Daten zu transportieren, zu speichern oder um mobil auf sie zugreifen zu können. Zu Wechseldatenträgern gehören externe Festplatten, CD-ROMs, DVDs, Speicherkarten, Magnetbänder und USB-Sticks.

Wechseldatenträger sind danach klassifizierbar, ob sie nur lesbar, einmalig beschreibbar oder wiederbeschreibbar sind. Unterschiede gibt es auch bei der Art der Datenspeicherung (analog oder digital) oder ihrer Bauform. So gibt es auswechselbare Datenträger (z. B. verbaute Festplatten) oder externe Datenspeicher (z. B. USB-Sticks).

1.2. Zielsetzung

In diesem Baustein wird aufgezeigt, wie Wechseldatenträger sicher genutzt werden können. Außerdem wird beschrieben, wie verhindert werden kann, dass über Wechseldatenträger unbeabsichtigt Informationen weitergegeben werden.

1.3. Abgrenzung und Modellierung

Der Baustein SYS.4.5 *Wechseldatenträger* ist auf jeden Wechseldatenträger im Informationsverbund anzuwenden.

Dieser Baustein beschäftigt sich mit den Sicherheitseigenschaften von Wechseldatenträgern. Der Schutz der IT-Systeme, an denen die Wechseldatenträger angeschlossen werden können, wird in dem vorliegenden Baustein nicht berücksichtigt. Empfehlungen hierzu sind in den Bausteinen SYS.1.1 *Allgemeiner Server* und SYS.2.1 *Allgemeiner Client* sowie den betriebssystemspezifischen Bausteinen zu finden.

Wechseldatenträger speichern Daten elektronisch, magnetisch oder auf andere, nicht direkt wahrnehmbare Weise. Sie verarbeiten dabei selbst keine Daten. Die Anforderungen an solche Geräte, wie z. B. Smartphones und Tablets, werden im Baustein SYS.3.2.1 *Allgemeine Smartphones und Tablets* aufgeführt. Nicht zu den Wechseldatenträgern zählen auch Cloud-Speicher. Anforderungen an Cloud-Umgebungen sind im Baustein OPS.2.2 *Cloud-Nutzung* zu finden.

Wechseldatenträger können bei persönlichen Treffen oder auch per Versand ausgetauscht werden. Der sichere Austausch der eigentlichen Informationen wird in diesem Baustein nicht betrachtet. Dazu sind die Anforderungen des Bausteins CON.9 *Informationsaustausch* zu erfüllen.

2. Gefährdungslage

Da IT-Grundschutz-Bausteine nicht auf individuelle Informationsverbünde eingehen können, werden zur Darstellung der Gefährdungslage typische Szenarien zugrunde gelegt. Die folgenden spezifischen Bedrohungen und Schwachstellen sind für den Baustein SYS.4.5 *Wechseldatenträger* von besonderer Bedeutung.

2.1. Sorglosigkeit im Umgang mit Informationen

Häufig gibt es in Institutionen zwar organisatorische Regelungen und technische Sicherheitsverfahren für Wechseldatenträger, diese werden jedoch oft durch einen sorglosen Umgang mit den Wechseldatenträgern umgangen. So kommt es etwa vor, dass Wechseldatenträger während einer Pause unbeaufsichtigt im Besprechungsraum zurück- oder auch im Zugabteil liegen gelassen werden.

2.2. Unzureichende Kenntnis über Regelungen

Wenn die Regelungen für den korrekten Umgang mit Wechseldatenträgern nicht hinreichend bekannt sind, können sie sich auch nicht eingehalten werden. So können zahlreiche Gefährdungen hinsichtlich der Informationssicherheit eintreten, zum Beispiel, wenn nicht geprüfte USB-Sticks an die IT-Systeme der Institution angeschlossen werden.

2.3. Diebstahl oder Verlust von Wechseldatenträgern

Bei Wechseldatenträgern ist das Risiko von Datenverlusten höher als bei stationären IT-Systemen. Ursachen für Datenverluste sind etwa Diebstahl oder verlorengegangene Geräte. Die auf den Wechseldatenträgern abgelegten Informationen sind in diesen Fällen oft unwiederbringlich verloren. Außerdem können die Informationen Externen in die Hände fallen.

2.4. Defekte Datenträger

Wechseldatenträger sind aufgrund ihrer Größe und Anwendungsbereiche anfällig für Beschädigungen, Fehler oder Ausfälle. Ursache sind beispielsweise ständig wechselnde Einsatzumgebungen oder mechanische Einwirkungen.

2.5. Beeinträchtigung durch wechselnde Einsatzumgebung

Wechseldatenträger werden in sehr unterschiedlichen Umgebungen eingesetzt und sind dadurch vielen Gefährdungen ausgesetzt. Dazu gehören beispielsweise schädigende Umwelteinflüsse wie zu hohe oder zu niedrige Temperaturen und Staub oder Feuchtigkeit. Hinzu kommen beispielsweise Transportschäden. Ein weiterer wichtiger Aspekt ist, dass Wechseldatenträger oft in Bereichen mit unterschiedlichem Sicherheitsniveau benutzt werden.

2.6. Verbreitung von Schadsoftware

Wechseldatenträger werden oft benutzt, um Daten zwischen verschiedenen Geräten und dem Arbeitsplatzrechner auszutauschen. Schadsoftware könnte Daten auf den Wechseldatenträgern kompromittieren und sich so auf die Arbeitsplatzrechner übertragen.

3. Anforderungen

Im Folgenden sind die spezifischen Anforderungen des Bausteins SYS.4.5 *Wechseldatenträger* aufgeführt. Der oder die Informationssicherheitsbeauftragte (ISB) ist dafür zuständig, dass alle Anforderungen gemäß dem festgelegten Sicherheitskonzept erfüllt und überprüft werden. Bei strategischen Entscheidungen ist der oder die ISB stets einzubeziehen.

Im IT-Grundschutz-Kompendium sind darüber hinaus weitere Rollen definiert. Sie sollten besetzt werden, insofern dies sinnvoll und angemessen ist.

Zuständigkeiten	Rollen
Grundsätzlich zuständig	IT-Betrieb
Weitere Zuständigkeiten	Fachverantwortliche, Benutzende

Genau eine Rolle sollte *Grundsätzlich zuständig* sein. Darüber hinaus kann es noch *Weitere Zuständigkeiten* geben. Falls eine dieser weiteren Rollen für die Erfüllung einer Anforderung vorrangig zuständig ist, dann wird diese Rolle hinter der Überschrift der Anforderung in eckigen Klammern aufgeführt. Die Verwendung des Singulars oder Plurals sagt nichts darüber aus, wie viele Personen diese Rollen ausfüllen sollen.

3.1. Basis-Anforderungen

Die folgenden Anforderungen MÜSSEN für diesen Baustein vorrangig erfüllt werden.

SYS.4.5.A1 Sensibilisierung zum sicheren Umgang mit Wechseldatenträgern (B)

Alle Benutzenden MÜSSEN für den sicheren Umgang mit Wechseldatenträgern sensibilisiert werden. Die Institution MUSS insbesondere darauf hinweisen, wie die Benutzenden mit Wechseldatenträgern umgehen sollten, um einem Verlust oder Diebstahl vorzubeugen und eine lange Lebensdauer zu gewährleisten.

Die Institution MUSS die Benutzenden darüber informieren, dass sie keine Wechseldatenträger, die aus unbekannten Quellen stammen, an ihre IT-Systeme anschließen dürfen.

SYS.4.5.A2 Verlust- und Manipulationsmeldung (B) [Benutzende]

Die Benutzenden MÜSSEN umgehend melden, wenn ein Wechseldatenträger gestohlen oder verloren wurde oder der Verdacht einer Manipulation besteht. Die Benutzenden MÜSSEN bei ihrer Meldung angeben, welche Informationen auf dem Wechseldatenträger gespeichert sind. Hierfür MUSS es in der Institution klare Meldewege und Zuständigkeiten geben.

Die Institution MUSS festlegen, wie Wechseldatenträger behandelt werden sollen, die nach einem Verlust wiedergefunden wurden. Wiedergefundene Wechseldatenträger DÜRFEN NICHT ohne vorherige Überprüfung auf Manipulation und Schadsoftware verwendet werden.

SYS.4.5.A3 ENTFALLEN (B)

Diese Anforderung ist entfallen.

SYS.4.5.A10 Datenträgerverschlüsselung (B)

Wenn Wechseldatenträger außerhalb eines sicheren Bereiches verwendet oder transportiert werden und dabei schutzbedürftige Daten enthalten, MÜSSEN die Daten mit einem sicheren Verfahren verschlüsselt werden.

SYS.4.5.A12 Schutz vor Schadsoftware (B) [Benutzende]

Die Institution MUSS sicherstellen, dass nur Daten auf Wechseldatenträger übertragen werden, die auf Schadsoftware überprüft wurden. Bevor Daten von Wechseldatenträgern verarbeitet werden, MÜSSEN sie auf Schadsoftware überprüft werden.

3.2. Standard-Anforderungen

Gemeinsam mit den Basis-Anforderungen entsprechen die folgenden Anforderungen dem Stand der Technik für diesen Baustein. Sie SOLLTEN grundsätzlich erfüllt werden.

SYS.4.5.A4 Erstellung einer Richtlinie zum sicheren Umgang mit Wechseldatenträgern (S)

Es SOLLTE eine Richtlinie für den richtigen Umgang mit Wechseldatenträgern erstellt werden. Folgende grundlegenden Aspekte SOLLTEN dabei berücksichtigt werden:

- welche Wechseldatenträger genutzt werden und wer diese einsetzen darf,
- welche Daten auf Wechseldatenträgern gespeichert werden dürfen und welche nicht,
- wie die auf Wechseldatenträgern gespeicherten Daten vor unbefugtem Zugriff, Manipulation und Verlust geschützt werden,
- wie die Daten auf den Wechseldatenträgern gelöscht werden sollen,
- mit welchen externen Institutionen Wechseldatenträger ausgetauscht werden dürfen und welche Sicherheitsregelungen dabei zu beachten sind,
- ob Wechseldatenträger an fremde IT-Systeme angeschlossen werden dürfen und was dabei zu beachten ist,
- wie Wechseldatenträger zu versenden sind sowie
- wie der Verbreitung von Schadsoftware über Wechseldatenträger vorgebeugt wird.

Die Institution SOLLTE in der Sicherheitsrichtlinie festlegen, unter welchen Bedingungen Wechseldatenträger gelagert werden sollen. Insbesondere SOLLTE die Institution vorgeben, dass nur berechtigte Benutzende Zugang zu beschriebenen Wechseldatenträgern haben. Die Institution SOLLTE festlegen, dass Angaben des herstellenden Unternehmens zum Umgang mit Datenträgern berücksichtigt werden müssen.

Die Institution SOLLTE die Verwendung von privaten Wechseldatenträgern untersagen.

Es SOLLTE regelmäßig überprüft werden, ob die Sicherheitsvorgaben für den Umgang mit Wechseldatenträgern aktuell sind.

SYS.4.5.A5 Regelung zur Mitnahme von Wechseldatenträgern (S)

Es SOLLTE klare schriftliche Regeln dazu geben, ob, wie und zu welchen Anlässen Wechseldatenträger mitgenommen werden dürfen. Insbesondere SOLLTE festgelegt sein, welche Wechseldatenträger von wem außer Haus transportiert werden dürfen und welche Sicherheitsmaßnahmen dabei zu beachten sind.

SYS.4.5.A6 Datenträgerverwaltung (S) [Fachverantwortliche]

Es SOLLTE eine Verwaltung für Wechseldatenträger geben. Die Wechseldatenträger SOLLTEN einheitlich gekennzeichnet werden. Die Verwaltung für Wechseldatenträger SOLLTE gewährleisten, dass Wechseldatenträger sachgerecht behandelt und aufbewahrt sowie ordnungsgemäß eingesetzt und transportiert werden.

SYS.4.5.A7 Sicheres Löschen der Wechseldatenträger vor und nach der Verwendung (S) [Fachverantwortliche]

Bevor Wechseldatenträger weitergegeben, wiederverwendet oder ausgesondert werden, SOLLTEN sie in geeigneter Weise sicher gelöscht werden.

SYS.4.5.A8 ENTFALLEN (S)

Diese Anforderung ist entfallen.

SYS.4.5.A13 Kennzeichnung der Wechseldatenträger beim Versand (S)

Wechseldatenträger, die versendet werden sollen, SOLLTEN so gekennzeichnet werden, dass die Absendenden und die Empfangenden sie sofort identifizieren können. Die Kennzeichnung der Wechseldatenträger oder deren Verpackung SOLLTE für die Empfangenden eindeutig sein. Die Kennzeichnung von Wechseldatenträgern mit schützenswerten Informationen SOLLTE für Außenstehende keine Rückschlüsse auf Art und Inhalte der Informationen zulassen.

SYS.4.5.A17 Gewährleistung der Integrität und Verfügbarkeit bei Langzeitspeichern (S)

Falls Wechseldatenträger verwendet werden, um Daten für lange Zeiträume zu speichern, SOLLTE die Institution sicherstellen, dass die verwendeten Wechseldatenträger geeignet sind, um die Integrität und Verfügbarkeit der Daten während des gesamten Nutzungszeitraums sicherzustellen. Die Integrität der Daten SOLLTE regelmäßig überprüft werden.

3.3. Anforderungen bei erhöhtem Schutzbedarf

Im Folgenden sind für diesen Baustein exemplarische Vorschläge für Anforderungen aufgeführt, die über dasjenige Schutzniveau hinausgehen, das dem Stand der Technik entspricht. Die Vorschläge SOLLTEN bei erhöhtem Schutzbedarf in Betracht gezogen werden. Die konkrete Festlegung erfolgt im Rahmen einer individuellen Risikoanalyse.

SYS.4.5.A9 ENTFALLEN (H)

Diese Anforderung ist entfallen.

SYS.4.5.A11 Integritätsschutz durch Checksummen oder digitale Signaturen (H)

Es SOLLTE ein Verfahren zum Schutz gegen zufällige oder vorsätzliche Veränderungen eingesetzt werden, mit dem die Integrität von vertraulichen Informationen sichergestellt wird. Die Verfahren zum Schutz vor Veränderungen SOLLTEN dem aktuellen Stand der Technik entsprechen.

SYS.4.5.A14 Sichere Versandart und Verpackung (H)

Die Institution SOLLTE überprüfen, wie vertrauliche Informationen bei einem Versand angemessen geschützt werden können. Es SOLLTE eine sichere Versandverpackung für Wechseldatenträger verwendet werden, bei der Manipulationen sofort zu erkennen sind. Die Institution SOLLTE alle Beteiligten auf notwendige Versand- und Verpackungsarten hinweisen.

SYS.4.5.A15 Verwendung zertifizierter Wechseldatenträger (H)

Die Institution SOLLTE nur Wechseldatenträger verwenden, die zertifiziert sind. Die Zertifizierung SOLLTE insbesondere eine integere Datenerhaltung sowie möglicherweise vorhandene Verschlüsselungsverfahren umfassen.

SYS.4.5.A16 Nutzung dedizierter IT-Systeme zur Datenprüfung (H)

Die Institution SOLLTE dedizierte IT-Systeme als Datenschleuse verwenden, bei denen Daten von einem Wechseldatenträger auf einen anderen übertragen werden und dabei auf Schadsoftware untersucht werden.

4. Weiterführende Informationen

4.1. Wissenswertes

Die International Organization for Standardization beschreibt in der Norm ISO/IEC 27001:2013 in Kapitel A.8.3 wie Wechseldatenträger sicher eingesetzt werden können.

IND: Industrielle IT

Bundesamt
für Sicherheit in der
Informationstechnik

IND.1 Prozessleit- und Automatisierungstechnik

1. Beschreibung

1.1. Einleitung

Prozessleit- und Automatisierungstechnik (Operational Technology, OT) ist Hard- und Software, die physische Geräte, Prozesse und Ereignisse in der Institution überwacht und steuert.

In der Industrie, zu der unter anderem auch die Kritischen Infrastrukturen gehören, zählen dazu insbesondere industrielle Steuerungssysteme (Industrial Control Systems, ICS) und Automationslösungen, die dort Steuerungs- und Regelfunktionen aller Art übernehmen. Weitere Beispiele sind Laborgeräte, z. B. automatisierte Mikroskope oder Analysewerkzeuge, Logistiksysteme, wie Barcodescanner mit Kleinrechner, oder Gebäudeleittechnik.

Die in der Vergangenheit übliche physische Trennung der OT von anderen IT-Systemen und Datennetzen in Büroanwendungen ist heute aufgrund zunehmender Integrationsanforderungen nur in Ausnahmefällen bei erhöhtem Schutzbedarf anwendbar. Mehrstufige Produktionsschritte und deren übergreifende Steuerung sowie regulatorische Anforderungen machen es zunehmend notwendig, die OT auch über Organisationsgrenzen hinweg zu öffnen. Diese Entwicklung wird durch den Trend zur Optimierung von Fertigungsprozessen noch beschleunigt, vor allem im Rahmen der Industrie 4.0.

Da in der OT zunehmend auch IT-Komponenten aus der Office-IT eingesetzt werden, ist diese inzwischen ähnlich gefährdet. Gleichzeitig weist die OT gegenüber der klassischen IT aber wesentliche Unterschiede auf, die es erschweren, dort etablierte Sicherheitsverfahren anzuwenden. So kann es aufgrund von Vorgaben der herstellenden Unternehmen oder gesetzlichen Anforderungen Beschränkungen geben, die Veränderungen an Komponenten verhindern oder erschweren, wie zum Beispiel das Einspielen von Sicherheitsupdates oder nachträgliche Härtungsmaßnahmen. Die OT unterliegt zudem in der Regel deutlich längeren Lebenszyklen, auch über die Unterstützung der herstellenden Unternehmen hinaus, sodass Sicherheitsupdates nicht durchgängig verfügbar sind.

Ein wesentlicher Unterschied ergibt sich für die OT auch aus den oft hohen Verfügbarkeits- und Integritätsanforderungen. Denn im Vergleich dazu ist bei der Office-IT die Verfügbarkeit häufig von nachrangiger Bedeutung. Störungen von OT-Systemen können dagegen Gefährdungen von Leib, Leben und Umwelt nach sich ziehen und sind zumeist nicht durch einen Neustart zu beheben.

1.2. Zielsetzung

Ziel dieses Bausteins ist es, geeignete Anforderungen an die Informationssicherheit der OT aufzuzeigen. Er enthält komponentenübergreifende, konzeptionelle und architektonische Sicherheitsanforderungen.

1.3. Abgrenzung und Modellierung

Der Baustein IND.1 *Prozessleit- und Automatisierungstechnik* ist auf jedes IT-System mit Prozessleit- und Automatisierungstechnik innerhalb des Informationsverbunds mindestens einmal anzuwenden.

Der Baustein ist übergreifend umzusetzen. Bestehen in den einzelnen Bereichen mit Prozessleit- und Automatisierungstechnik unterschiedliche Sicherheitsanforderungen an die Informationssicherheit, sollte der Baustein auf jedes IT-System getrennt angewandt werden.

Die Ausgestaltung der OT kann je nach Zweck, Branche, den eingesetzten IT-Systemen und der Technik sowie aufgrund des langen Einsatzzeitraums selbst bei vergleichbaren Anwendungsfällen stark variieren. Werden die Sicherheitsmaßnahmen auf Basis der Anforderungen aus diesem Baustein ausgewählt, sind diese Besonderheiten dabei zu berücksichtigen. Sie können wesentlichen Einfluss auf die Ausgestaltung des Sicherheitskonzepts nehmen.

Auch der Risikoanalyse kann aus diesem Grund bereits bei der Erstellung eines Sicherheitskonzepts für den normalen Schutzbedarf eine hohe Bedeutung zukommen.

Das Betriebspersonal sollte in Bezug auf relevante Bedrohungen und Gefährdungen geschult und sensibilisiert werden. Hierfür ist der Baustein ORP.3 *Sensibilisierung und Schulung zur Informationssicherheit* umzusetzen.

Zusätzlich zu diesem Baustein ist die umgebende Infrastruktur der OT, also Standorte, Anlagen, Gebäude oder Räume, durch möglichst spezifische Bausteine zu modellieren, um die Schutzwirkung dieses Bausteins zu ergänzen.

Für eine geeignete Protokollierung im Bereich der Prozessleit- und Steuerungstechnik ist der Baustein OPS.1.1.5 *Protokollierung* umzusetzen.

ICS-Systeme sollten grundsätzlich mit berücksichtigt werden, wenn der Baustein ORP.4 *Identitäts- und Berechtigungsmanagement* umgesetzt wird.

2. Gefährdungslage

Da IT-Grundschutz-Bausteine nicht auf individuelle Informationsverbünde eingehen können, werden zur Darstellung der Gefährdungslage typische Szenarien zugrunde gelegt. Die folgenden spezifischen Bedrohungen und Schwachstellen sind für den Baustein IND.1 *Prozessleit- und Automatisierungstechnik* von besonderer Bedeutung.

2.1. Beeinträchtigung durch schädliche Umgebungseinflüsse

ICS-Komponenten sind in industriellen Umgebungen häufig besonderen Bedingungen ausgesetzt, die den sicheren Betrieb beeinträchtigen können. Dazu zählen extreme Wärme, Kälte, Feuchtigkeit, Staub, Vibration oder auch ätzend oder korrodierend wirkende Umgebungen. Häufig treten auch mehrere Faktoren gleichzeitig auf. Durch solche schädlichen Einflüsse können ICS-Komponenten schneller verschleißen und früher ausfallen.

2.2. Ungeeignete Einbindung der OT in die Sicherheitsorganisation

Durch unterschiedliche Rahmenbedingungen, Kenntnisse und Vorgehensweisen in den Bereichen Office-IT und OT können bei übergreifenden Sicherheitsvorgaben Probleme bei der Umsetzung auftreten. Sicherheitsvorgaben aus dem Bereich der Office-IT können einerseits aufgrund technischer oder prozessualer Besonderheiten bei ICS-Systemen nicht umsetzbar sein. Andererseits könnte es sein, dass ICS-spezifische Informationssicherheits- und Safety-Aspekte, also Aspekte der funktionalen Sicherheit, den oder der Informationssicherheitsbeauftragten der Office-IT nicht bekannt sind. So können Reibungsverluste in der Kommunikation und der Umsetzung entstehen. Außerdem könnten Risiken nicht erkannt oder unzureichend behandelt werden.

2.3. Ungeeignete Einbindung der OT in betriebliche Abläufe

Auch wenn sich OT und IT zunehmend annähern, gibt es Besonderheiten, die das Übertragen etablierter betrieblicher Abläufe erschweren. Betriebliche Eingriffe im Rahmen des Change- und Incident-Managements zur sicheren Konfiguration, Störungsbehebung oder zum Einspielen von Sicherheitsupdates können etwa eine erneute behördliche Freigabe oder den Verlust des Supports nach sich ziehen. Nicht autorisierte Änderungen können die Funktion einer Komponente beeinflussen und damit potenziell auch Auswirkungen auf deren Safety-Funktion haben.

Die OT dient der Überwachung, Steuerung und Automatisierung von technischen Abläufen. Störungen dieser Systeme können zu Produktionsausfällen, technischen oder personellen Schäden und Umweltschäden führen. Diese potenziellen Auswirkungen müssen bei betrieblichen Eingriffen berücksichtigt werden.

2.4. Unzureichender Zugangsschutz

Industrielle Steuerungsanlagen werden immer seltener vollständig autark von der Außenwelt betrieben. Moderne Fertigungs- und Erzeugungsprozesse erfordern einen Informationsaustausch mit vor- und nachgelagerten Produktionsschritten und sind häufig an die zentralen Produktionsplanungs- und Steuerungssysteme einer Institution angebunden. Um elektronisch Informationen auszutauschen, müssen die Produktionsanlagen außerdem mit Drittnetzen, wie der Office-IT oder den Netzen von Partnern, Partnerinnen und Dienstleistenden, verbunden sein. Interaktive Zugriffe von Büro- oder Mobilarbeitsplätzen und der betrieblich bedingte elektronische Datenaustausch, etwa zur Bereitstellung von Software und Updates, bedeuten eine weitere Vernetzung mit der Außenwelt. Auch die Einrichtung von Fernzugängen für eine Rufbereitschaft oder für Dienstleistende können den Zugriff von außen ermöglichen.

Werden die erforderlichen Kommunikationskanäle zu weit gefasst oder unzureichend gesichert, können Dritte diese Zugangswege ausnutzen, um auf diese zuzugreifen und um diese zu kompromittieren. Industrielle Steuerungsanlagen können einerseits von zielgerichteten Schadsoftware-Angriffen betroffen sein. Andererseits können sie auch von Schadprogrammen kompromittiert werden, die eigentlich auf die Manipulation der Office-IT abzielen. Durch eine fehlende Segmentierung oder Kontrolle des Datenverkehrs kann Schadsoftware auf die Systeme gelangen.

Aber auch der Einsatz von Virenschutz-Software kann ein Risiko für die OT darstellen. Etwa dann, wenn keine Freigabe des herstellenden Unternehmens für die Umgebung vorliegt oder Fehlerkennungen und aktive Systemeingriffe den Betrieb gefährden. Ein vergleichbares Störungspotenzial kann sich auch aus dem Betrieb netzbasierter Intrusion Prevention Systeme (IPS) ergeben, weil dabei Verbindungen unterbrochen werden können.

2.5. Unsicherer Projektierungsprozess/Anwendungsentwicklungsprozess

Anpassungen und Weiterentwicklungen von IT-Systemen, Anwendungen und Steuerungsprogrammen können einen kritischen Eingriff in die Steuerungsanlage darstellen. Störungen können dabei aus funktionalen Fehlern bei unzureichenden Test- und Validierungsschritten, fehlerhaften oder manipulierten Projektierungsdaten oder Schwachstellen in der Software entstehen. Etwa dann, wenn wichtige Sicherheitsfunktionen wie Ein- und Ausgabe- oder Berechtigungsprüfungen unzureichend umgesetzt werden.

Weitere Gefahren können sich aus unsicheren Entwicklungsumgebungen, der ungeeigneten Ablage von Programmcode, Dokumentations- oder Projektdaten sowie aus den Datentransferschnittstellen ergeben.

2.6. Unsicheres Administrationskonzept und Fernadministration

Die Administration industrieller Steuerungssysteme erfolgt in bestimmten Fällen über Netzzugriffe. Dabei werden unterschiedliche öffentliche und private Netze wie z. B. Telefonnetze, Funknetze, Mobilfunknetze und zunehmend das Internet genutzt. Sind diese Zugänge unzureichend geplant, unsicher konfiguriert oder werden diese nicht überwacht, können Dritte unter Umständen unbefugt auf einzelne OT-Komponenten oder die Infrastruktur zugreifen. So können sie etwa die Sicherheitsmechanismen am Perimeter umgehen.

2.7. Unzureichende Überwachungs- und Detektionsverfahren

Eine wesentliche Funktion industrieller Steuerungssysteme ist es, den Betrieb eines automatisierten Prozesses zu überwachen. So wird etwa bei unterschrittenen Füllständen oder abweichenden Temperaturen oder Ventilstellungen eine entsprechende Warnung ausgegeben. Die unterstützende IT-Infrastruktur wird dagegen häufig nicht ausreichend überwacht.

Werden ungewöhnliche oder sicherheitsrelevante Ereignisse solcher Betriebsumgebungen nicht oder nur unzureichend kontrolliert, können Angriffsversuche, Netzengpässe oder absehbare Ausfälle nicht frühzeitig erkannt werden. Darüber hinaus kann auch eine mangelhafte Auswertung oder eine unübersichtliche Darstellung der Ereignisse dazu führen, dass Warnungen und Fehler verspätet erkannt werden.

2.8. Unzureichendes Testkonzept

Industrielle Steuerungsanlagen unterliegen oft hohen Verfügbarkeitsanforderungen. Denn Störungen oder technische Ausfälle können unter Umständen schwerwiegende Schäden und hohe Folgekosten nach sich ziehen. Aus diesem Grund sind OT-Systeme oft ausfallsicher konzipiert.

Werden Änderungen an einer solchen Umgebung nicht sorgfältig geplant, abgestimmt und in einer realitätsnahen Umgebung getestet, besteht die Gefahr, dass logische oder softwaretechnische Fehler übersehen werden und Störungen in der Anlage auftreten. Selbst vom herstellenden Unternehmen freigegebene Updates können bei der Modifikation oder Anpassung von Parametern Störungen an der Anlage verursachen.

2.9. Mangelnde Life-Cycle-Konzepte

Neben spezifischen ICS-Komponenten werden zunehmend Komponenten und Software aus der Office-IT eingesetzt. Aufgrund der sehr langen Lebenszyklen in der OT werden diese Komponenten in der Regel deutlich länger betrieben als in der Office-IT üblich, teilweise auch über die Support-Zyklen der herstellenden Unternehmen hinaus.

Dies hat zur Folge, dass nach dem Ablauf der Unterstützung der herstellenden Unternehmen keine Updates gegen Schwachstellen mehr zur Verfügung gestellt werden. Dem gegenüber stehen oftmals öffentlich dokumentierte

Schwachstellen sowie Werkzeuge, die diese Schwachstellen ausnutzen. Dies ermöglicht auch nicht versierten Angreifenden ein erfolgreiches Eindringen in die OT-Systeme. Das gilt auch, wenn Updates nicht oder nur mit sehr großer Verzögerung eingespielt werden.

Die langen Einsatzzeiten können zudem zu Problemen bei der Beschaffung von Ersatzteilen führen, etwa wenn diese nicht mehr produziert werden. Dies gilt auch für mögliches Know-how zur Pflege und Wartung von Alt-Systemen, über das neue Mitarbeitende nicht mehr verfügen.

Zudem enthalten ICS-Komponenten häufig detaillierte Informationen über den geregelten oder überwachten Prozess. Auch aus sonstigen übertragenen Werten, wie Mess- oder Steuerungsdaten, lassen sich diese Informationen teilweise rekonstruieren. Gleiches gilt für Steuerungsprogramme oder -parameter. Angreifende könnten so an Geschäftsgeheimnisse gelangen.

2.10. Unzureichende Sicherheitsanforderungen bei der Beschaffung

Aufgrund nicht ausreichender Sicherheitsanforderungen und aus Kostengründen wird bei der Beschaffung häufig die Informationssicherheit nicht berücksichtigt. Dadurch können in ICS-Komponenten mitunter schwerwiegende Schwachstellen, z. B. in Hardware oder Software enthalten sein, die sich später nur sehr aufwändig beheben lassen.

2.11. Einsatz unsicherer Protokolle

Die ICS-Komponenten kommunizieren untereinander über verschiedene Netzprotokolle und Standards. Neben Protokollen und Standards aus der Office-IT wie Ethernet, TCP/IP, WLAN oder GSM werden OT-spezifische Protokolle eingesetzt. Diese sind nicht immer unter dem Gesichtspunkt der Informationssicherheit entwickelt worden und bieten demgemäß teilweise keine oder nur eingeschränkte Sicherheitsmechanismen. Informationen werden häufig im Klartext und ohne Integritätssicherung oder Authentisierung übertragen.

Angreifende mit Zugang zum Netz könnte die Inhalte der Kommunikation auslesen oder verändern und auf diese Weise die Prozesse beeinflussen, etwa indem Sensordaten vorgetäuscht oder Steuerungsbefehle gefälscht werden. Dies trifft in besonderem Maße auf Protokolle zu, die für die Kommunikation über frei zugängliche Gebiete eingesetzt werden, etwa bei Funkprotokollen oder im Rahmen der Standortvernetzung.

2.12. Unsichere Konfigurationen von ICS-Komponenten

In der Standardkonfiguration von ICS-Komponenten werden Sicherheitsmaßnahmen nicht immer aktiviert. Dadurch können Unbefugte leicht Zugriff erlangen. Der Betrieb unsicher konfigurierter Komponenten kann darüber hinaus auch die Sicherheit anderer Komponenten der Umgebung bedrohen, etwa wenn Zugangsdaten zu diesen ausgelesen werden können oder sie in einer Vertrauensstellung zu anderen Systemen stehen.

Beispielsweise könnten Standardpasswörter gebraucht, Klartextprotokolle zur Systemverwaltung genutzt, nicht erforderliche Dienste betrieben, ungesicherte Schnittstellen wie z. B. USB- oder Firewire-Ports verwendet oder Sicherheitsfunktionen deaktiviert werden.

2.13. Abhängigkeiten der OT von IT-Netzen

Die OT wird mittlerweile immer weniger völlig autark betrieben. Bestehen Abhängigkeiten zu anderen Systemen, Netzen oder Diensten, wirken sich Ausfälle oder Sicherheitsvorfälle im IT-Netz auch auf die OT aus.

Insbesondere wenn diese Systeme und Netze nicht unter der direkten Kontrolle des Betreibenden stehen, kann die Verfügbarkeit der OT und seiner Prozesse stark beeinträchtigt werden. Darüber hinaus kann ein Vorfall oder Fehler in der Regel nur mit externer Unterstützung behoben werden.

Beispiele für Abhängigkeiten zu anderen Systemen und Netzen sind Internetanbindungen, gemeinsam genutzte Infrastrukturkomponenten, eine Betriebsführung und Überwachung durch Dienstleistende oder die Nutzung von Cloud-Diensten.

3. Anforderungen

Im Folgenden sind die spezifischen Anforderungen des Bausteins IND.1 *Prozessleit- und Automatisierungstechnik* aufgeführt. Der oder die Informationssicherheitsbeauftragte (ISB) ist dafür zuständig, dass alle Anforderungen gemäß dem festgelegten Sicherheitskonzept erfüllt und überprüft werden. Bei strategischen Entscheidungen ist der oder die ISB stets einzubeziehen.

Im IT-Grundschutz-Kompendium sind darüber hinaus weitere Rollen definiert. Sie sollten besetzt werden, insofern dies sinnvoll und angemessen ist.

Zuständigkeit	Rolle
Grundsätzlich zuständig	ICS-Informationssicherheitsbeauftragte
Weitere Zuständigkeiten	Mitarbeitende, Planende, IT-Betrieb, OT-Betrieb (Operational Technology, OT)

Genau eine Rolle sollte *Grundsätzlich zuständig* sein. Darüber hinaus kann es noch *Weitere Zuständigkeiten* geben. Falls eine dieser weiteren Rollen für die Erfüllung einer Anforderung vorrangig zuständig ist, dann wird diese Rolle hinter der Überschrift der Anforderung in eckigen Klammern aufgeführt. Die Verwendung des Singulars oder Plurals sagt nichts darüber aus, wie viele Personen diese Rollen ausfüllen sollen.

3.1. Basis-Anforderungen

Die folgenden Anforderungen MÜSSEN für diesen Baustein vorrangig erfüllt werden.

IND.1.A1 Einbindung in die Sicherheitsorganisation (B)

Ein Managementsystem für Informationssicherheit (ISMS) für den Betrieb der OT-Infrastruktur MUSS entweder als selbständiges ISMS oder als Teil eines Gesamt-ISMS existieren.

Eine gesamtverantwortliche Person für die Informationssicherheit im OT-Bereich MUSS benannt werden. Er oder sie MUSS innerhalb der Institution bekannt gegeben werden.

IND.1.A2 ENTFALLEN (B)

Diese Anforderung ist entfallen.

IND.1.A3 Schutz vor Schadprogrammen (B)

Beim Einsatz von Virenschutz-Software auf OT-Komponenten MUSS berücksichtigt werden, ob und in welcher Konfiguration der Betrieb von Virenschutz-Software vom herstellenden Unternehmen unterstützt wird. Ist dies nicht der Fall, MUSS der Bedarf an alternativen Schutzverfahren geprüft werden.

Die Virensignaturen DÜRFEN NICHT von OT-Systemen direkt aus dem Internet bezogen werden.

IND.1.A18 Protokollierung (B) [OT-Betrieb (Operational Technology, OT)]

Jede Änderung an ICS-Komponenten MUSS protokolliert werden. Außerdem MÜSSEN alle Zugriffe auf ICS-Komponenten protokolliert werden.

IND.1.A19 Erstellung von Datensicherungen (B) [Mitarbeitende, OT-Betrieb (Operational Technology, OT)]

Programme und Daten MÜSSEN regelmäßig gesichert werden. Auch nach jeder Systemänderung an OT-Komponenten MUSS eine Sicherung erstellt werden.

3.2. Standard-Anforderungen

Gemeinsam mit den Basis-Anforderungen entsprechen die folgenden Anforderungen dem Stand der Technik für diesen Baustein. Sie SOLLTEN grundsätzlich erfüllt werden.

IND.1.A4 Dokumentation der OT-Infrastruktur (S)

Alle sicherheitsrelevanten Parameter der OT-Infrastruktur SOLLTEN dokumentiert sein. In einem Bestandsverzeichnis SOLLTEN alle Software- und Systemkomponenten geführt werden. Hieraus SOLLTEN die eingesetzten Produkt- und Protokollversionen sowie die Zuständigkeiten hervorgehen. Zu den eingesetzten Komponenten SOLLTEN eventuelle Restriktionen der herstellenden Unternehmen oder regulatorische Auflagen bestimmt sein. Diese Dokumentation und ein Systeminventar SOLLTEN beispielsweise in einem Leitsystem geführt werden.

Zusätzlich SOLLTE ein aktueller Netzplan Zonen, Zonenübergänge (Conduits), eingesetzte Kommunikationsprotokolle und -verfahren sowie Außenschnittstellen dokumentieren. Bei den Schnittstellen SOLLTEN aktive Netzkomponenten und manuelle Datentransferverfahren, z. B. durch Wechseldatenträger, berücksichtigt werden. Zonen und Conduits schützen die OT-Infrastrukur, indem die Automatisierungslösung in Zellen und Kommunikationskanälen strukturiert werden SOLLTE.

IND.1.A5 Entwicklung eines geeigneten Zonenkonzepts (S) [Planende]

Die OT-Infrastruktur SOLLTE auch horizontal in unabhängige Funktionsbereiche, wie etwa Anlagen, segmentiert werden. Die einzelnen Zonen SOLLTEN, so weit wie möglich, im Betrieb voneinander unabhängig sein. Insbesondere die Zonen, in denen der technische Prozess gesteuert wird, SOLLTEN bei einem Ausfall der anderen Zonen für einen gewissen Zeitraum weiter funktionstüchtig sein. Auch SOLLTE die Abkopplung nach einem Angriff weiter funktionieren. Dieser Zeitraum SOLLTE geeignet definiert und dokumentiert werden. Das Netz SOLLTE manipulations- und fehlerresistent konzipiert werden.

IND.1.A6 Änderungsmanagement im OT-Betrieb (S)

Für Änderungen an der OT SOLLTE ein eigener Änderungsprozess definiert, dokumentiert und gelebt werden.

IND.1.A7 Etablieren einer übergreifenden Berechtigungsverwaltung zwischen der OT und in der Office-IT (S)

Die Institution SOLLTE einen Prozess zur Verwaltung von Zugängen und zugeordneten Berechtigungen für den Zugriff auf die OT etablieren. Die Berechtigungsverwaltung SOLLTE den Prozess, die Durchführung und die Dokumentation für die Beantragung, Einrichtung und den Entzug von Berechtigungen umfassen.

Die Berechtigungsverwaltung SOLLTE gewährleisten, dass Berechtigungen nach dem Minimalprinzip vergeben und regelmäßig überprüft werden. In der Berechtigungsverwaltung SOLLTEN die Zugriffe auf IT-Systeme für Mitarbeitende, Administrierende und Dritte geregelt sein. Jeder oder jede Beteiligte SOLLTE regelmäßig zu den einzuhaltenden Regelungen sensibilisiert werden. Die Einhaltung SOLLTE überprüft werden. Fehlverhalten SOLLTE sanktioniert werden.

IND.1.A8 Sichere Administration (S) [IT-Betrieb]

Für die Erstkonfiguration, Verwaltung und Fernwartung in der OT SOLLTEN entweder sichere Protokolle oder abgetrennte Administrationsnetze mit entsprechendem Schutzbedarf genutzt werden. Der Zugang zu diesen Schnittstellen SOLLTE auf die Berechtigten eingeschränkt sein. Es SOLLTE nur der Zugriff auf die Systeme und Funktionen gewährt sein, die für die jeweilige Administrationsaufgabe benötigt werden.

Die Systeme und Kommunikationskanäle, mit denen die Administration oder Fernwartung durchgeführt wird, SOLLTEN das gleiche Schutzniveau aufweisen wie die verwaltete OT-Komponente.

IND.1.A9 Restriktiver Einsatz von Wechseldatenträgern und mobilen Endgeräten in ICS-Umgebungen (S)

Für die Nutzung von Wechseldatenträgern und mobilen Endgeräten SOLLTEN Regelungen aufgestellt und bekannt gegeben werden. Der Einsatz von Wechseldatenträgern und mobilen Endgeräten in ICS-Umgebungen SOLLTE beschränkt werden. Für Medien und Geräte von Dienstleistenden SOLLTEN ein Genehmigungsprozess und eine Anforderungsliste existieren. Die Vorgaben SOLLTEN allen Dienstleistenden bekannt sein und von diesen schriftlich bestätigt werden.

Auf den OT-Komponenten SOLLTEN alle nicht benötigten Schnittstellen deaktiviert werden. An den aktiven Schnittstellen SOLLTE die Nutzung auf bestimmte Geräte oder Medien eingeschränkt werden.

IND.1.A10 Monitoring, Protokollierung und Detektion (S) [OT-Betrieb (Operational Technology, OT)]

Betriebs- und sicherheitsrelevante Ereignisse SOLLTEN zeitnah identifiziert werden. Hierzu SOLLTE ein geeignetes Log- und Event-Management entwickelt und umgesetzt werden. Das Log- und Event-Management SOLLTE angemessene Maßnahmen umfassen, um sicherheitsrelevante Ereignisse zu erkennen und zu erheben. Es SOLLTE zudem einen Reaktionsplan (Security Incident Response) enthalten.

Der Reaktionsplan SOLLTE Verfahren zur Behandlung von Sicherheitsvorfällen festlegen. Darin abgedeckt sein SOLLTEN die Klassifizierung von Ereignissen, Meldewege und Festlegung der einzubeziehenden Organisationseinheiten, Reaktionspläne zur Schadensbegrenzung, Analyse und Wiederherstellung von Systemen und Diensten sowie die Dokumentation und Nachbereitung von Vorfällen.

IND.1.A11 Sichere Beschaffung und Systementwicklung (S)

Sollen OT-Systeme beschafft, geplant oder entwickelt werden, SOLLTEN Regelungen zur Informationssicherheit getroffen und dokumentiert werden. Die Unterlagen SOLLTEN Teil der Ausschreibung sein.

Bei Beschaffungen, Planungen oder Entwicklungen SOLLTE die Informationssicherheit in dem gesamten Lebenszyklus berücksichtigt werden. Voraussetzungen und Umsetzungshinweise für einen sicheren Betrieb von ICS-Komponenten von den herstellenden Unternehmen SOLLTEN frühzeitig eingeplant und umgesetzt werden. Für ICS-Komponenten SOLLTEN einheitliche und dem Schutzbedarf angemessene Anforderungen an die Informationssicherheit definiert werden. Diese SOLLTEN berücksichtigt werden, wenn neue ICS-Komponenten beschafft werden. Die Einhaltung und Umsetzung SOLLTE dokumentiert werden.

Die Institution SOLLTE dokumentieren, wie sich das System in die Konzepte für die Zoneneinteilung, das Berechtigungs- und Schwachstellen-Management sowie für den Virenschutz einfügt und diese gegebenenfalls anpassen. Es SOLLTE geregelt sein, wie der Betrieb aufrechterhalten werden kann, falls einer der Kooperationspartner keine Dienstleistungen mehr anbietet.

IND.1.A12 Etablieren eines Schwachstellen-Managements (S)

Für den sicheren Betrieb einer OT-Umgebung SOLLTE die Institution ein Schwachstellen-Management etablieren. Das Schwachstellen-Management SOLLTE Lücken in Software, Komponenten, Protokollen und Außenschnittstellen der Umgebung identifizieren. Außerdem SOLLTEN sich daraus erforderliche Handlungen ableiten, bewerten und umsetzen lassen.

Grundlage dafür SOLLTEN Schwachstellenmeldungen von herstellenden Unternehmen oder öffentlich verfügbare CERT-Meldungen sein. Ergänzend hierzu SOLLTEN organisatorische und technische Audits zur Schwachstellenanalyse durchgeführt werden.

IND.1.A20 Systemdokumentation (S) [Mitarbeitende, OT-Betrieb (Operational Technology, OT)]

Es SOLLTE eine erweiterte Systemdokumentation erstellt werden. Darin SOLLTEN Besonderheiten im Betrieb und die Möglichkeiten zur Systemverwaltung festgehalten werden. Außerdem SOLLTE dokumentiert werden, wenn ICS-Komponenten verändert werden.

IND.1.A21 Dokumentation der Kommunikationsbeziehungen (S) [OT-Betrieb (Operational Technology, OT)]

Es SOLLTE dokumentiert werden, mit welchen Systemen eine ICS-Komponente welche Daten austauscht. Außerdem SOLLTEN die Kommunikationsverbindungen neu integrierter ICS-Komponenten dokumentiert werden.

IND.1.A22 Zentrale Systemprotokollierung und -überwachung (S) [OT-Betrieb (Operational Technology, OT)]

Die Protokollierungsdaten von ICS-Komponenten SOLLTEN zentral gespeichert werden. Bei sicherheitskritischen Ereignissen SOLLTE automatisch alarmiert werden.

IND.1.A23 Aussonderung von ICS-Komponenten (S) [OT-Betrieb (Operational Technology, OT)]

Wenn alte oder defekte ICS-Komponenten ausgesondert werden, SOLLTEN alle schützenswerten Daten sicher gelöscht werden. Es SOLLTE insbesondere sichergestellt sein, dass alle Zugangsdaten nachhaltig entfernt wurden.

3.3. Anforderungen bei erhöhtem Schutzbedarf

Im Folgenden sind für diesen Baustein exemplarische Vorschläge für Anforderungen aufgeführt, die über dasjenige Schutzniveau hinausgehen, das dem Stand der Technik entspricht. Die Vorschläge SOLLTEN bei erhöhtem Schutzbedarf in Betracht gezogen werden. Die konkrete Festlegung erfolgt im Rahmen einer individuellen Risikoanalyse.

IND.1.A13 Notfallplanung für OT (H)

Notfallpläne für den Ausfall und für die Kompromittierung jeder Zone SOLLTEN definiert, dokumentiert, nach jeder größeren Änderung getestet und regelmäßig geübt sein.

Zudem SOLLTE ein wirksames Ersatzverfahren für den Ausfall der (Fern-) Administrationsmöglichkeit definiert, dokumentiert und getestet sein.

IND.1.A14 Starke Authentisierung an OT-Komponenten (H)

Zur sicheren Authentisierung von privilegierten Benutzenden in Steuerungssystemen SOLLTE ein zentraler Verzeichnisdienst eingerichtet werden (siehe Baustein ORP.4 *Identitäts- und Berechtigungsmanagement*). Die Authentisierung SOLLTE durch den Einsatz mehrerer Faktoren wie Wissen, Besitz oder Biometrie zusätzlich abgesichert werden.

Bei der Planung SOLLTE darauf geachtet werden, dass daraus entstehende Abhängigkeiten in der Authentisierung bekannt sind und bei der Umsetzung der Lösung berücksichtigt werden.

Es SOLLTE sichergestellt werden, dass die Authentisierung von betrieblich erforderlichen technischen Konten auch in Notfällen durchgeführt werden kann.

IND.1.A15 Überwachung von weitreichenden Berechtigungen (H)

Die Institution SOLLTE ein Bestandsverzeichnis führen, das alle vergebenen Zutritts-, Zugangs und Zugriffsrechte auf kritische Systeme enthält. Das Verzeichnis SOLLTE beinhalten, welche Rechte ein bestimmter Benutzender oder eine bestimme Benutzende effektiv hat und wer an einem bestimmten System über welche Rechte verfügt.

Alle kritischen administrativen Tätigkeiten SOLLTEN protokolliert werden. Der IT-Betrieb SOLLTE NICHT die Protokolle löschen oder manipulieren können.

IND.1.A16 Stärkere Abschottung der Zonen (H)

Bei hoch schutzbedürftigen oder schlecht absicherbaren ICS-Umgebungen SOLLTEN vorbeugend Schnittstellensysteme mit Sicherheitsprüffunktionen eingesetzt werden.

Durch Realisierung einer oder mehrerer Anbindungszonen (DMZ) in P-A-P-Struktur SOLLTEN durchgängige Außenverbindungen terminiert werden. Erforderliche Sicherheitsprüfungen SOLLTEN so erfolgen, dass die ICS-Anlage nicht angepasst werden muss.

IND.1.A17 Regelmäßige Sicherheitsüberprüfung (H)

Die Sicherheitskonfiguration von OT-Komponenten SOLLTE regelmäßig und bedarfsorientiert bei plötzlich auftretenden neuen, bisher unbekannten Gefährdungen überprüft werden. Die Sicherheitsüberprüfung SOLLTE zumindest die exponierten Systeme mit Außenschnittstellen oder Benutzendeninteraktion umfassen. Auch das realisierte Sicherheitskonzept SOLLTE regelmäßig überprüft werden. Die Sicherheitsüberprüfung SOLLTE als Konfigurationsprüfung oder auch durch automatisierte Konformitätsprüfungen erfolgen.

IND.1.A24 Kommunikation im Störfall (H) [Mitarbeitende, OT-Betrieb (Operational Technology, OT)]

Alternative und unabhängige Kommunikationsmöglichkeiten SOLLTEN aufgebaut und betrieben werden.

4. Weiterführende Informationen

4.1. Wissenswertes

Das BSI hat mit dem Dokument „Empfehlungen für Fortbildungs- und Qualifizierungsmaßnahmen im ICS-Umfeld" entsprechende Hilfestellungen zur Absicherung im ICS-Umfeld veröffentlicht.

Mit dem „ICS Security Kompendium" gibt das Bundesamt für Sicherheit in der Informationstechnik (BSI) Hilfestellungen für den Test der Komponenten und Maßnahmen für die IT-Sicherheit in ICS für Herstellende und Integratoren von ICS.

Die International Organization for Standardization (ISO) macht in der Norm ISO/IEC 27019 „Information technology – Security techniques – Information security controls for the energy utility industry" Vorgaben für die Absicherung von Energieversorgern.

Der Bundesverband der Energie- und Wasserwirtschaft e. V. (BDEW) und Oesterreichs E-Wirtschaft bietet mit dem Dokument „Whitepaper: Anforderungen an sichere Steuerungs- und Telekommunikationssysteme" eine Hilfestellung zum sicheren Betrieb von Steuerungs- und Telekommunikationssystemen.

Die internationale Norm IEC 62443-2-1:2010 „Industrial communication networks – Network and system security: Part 2-1: Establishing an industrial automation and control system security program, International Electrotechnical Commission (IEC)", 2010, legt fest, was zur Einrichtung von IT-Sicherheit in Netzen und Systemen notwendig ist.

Bundesamt
für Sicherheit in der
Informationstechnik

IND.2.1 Allgemeine ICS-Komponente

1. Beschreibung

1.1. Einleitung

Eine ICS-Komponente ist eine elektronische Komponente, die eine Maschine oder Anlage steuert oder regelt. Sie ist damit Bestandteil eines industriellen Steuerungssystems (englisch Industrial Control System, ICS) oder allgemeiner einer Betriebstechnik (englisch Operational Technology, OT). Diese Komponenten können Speicherprogrammierbare Steuerungen (SPS) (englisch Programmable Logic Controller, PLC), Sensoren, Aktoren, eine Maschine oder andere Teile eines ICS sein.

Aufgrund der im OT-Umfeld typischen hohen Verfügbarkeitsanforderungen und der oft extremen Umgebungsbedingungen wie Hitze oder Kälte, Staub, Vibration oder Korrosion wurden ICS-Komponenten schon immer als robuste Geräte mit hoher Zuverlässigkeit und langer Lebensdauer konstruiert.

ICS-Komponenten werden normalerweise über Spezialsoftware des jeweiligen herstellenden Unternehmens konfiguriert bzw. programmiert. Das wird entweder über sogenannte Programmiergeräte z. B. als Anwendung unter Windows oder Linux oder über eine Engineering-Station durchgeführt, welche die Anwendungsprogramme in die Speicherprogrammierbaren Steuerungen lädt.

Die Rolle des oder der Informationssicherheitsbeauftragten für den Bereich der industriellen Automatisierung wird je nach Art und Ausrichtung der Institution anders genannt. Eine weitere Bezeichnung neben ICS-Informationssicherheitsbeauftragte (ICS-ISB) ist auch Industrial Security Officer.

1.2. Zielsetzung

Ziel dieses Bausteins ist die Absicherung aller Arten von ICS-Komponenten, unabhängig von herstellenden Unternehmen, Bauart, Einsatzzweck und -ort. Er kann für ein einzelnes Gerät oder ein aus mehreren Komponenten aufgebautes modulares Gerät verwendet werden.

1.3. Abgrenzung und Modellierung

Der Baustein IND.2.1 *Allgemeine ICS-Komponente* ist auf jede im Informationsverbund eingesetzte ICS-Komponente anzuwenden.

Die Anforderungen sind für eine allgemeine ICS-Komponente erarbeitet. Für spezifischere ICS-Komponenten, z. B. Sensoren und Aktoren oder Maschinen, sind zusätzliche Bausteine wie IND.2.3 *Sensoren und Aktoren* bzw. IND.2.4 *Maschine* verfügbar. Dort sind Anforderungen beschrieben, die über die allgemeinen Anforderungen dieses Bausteins hinausgehen und zusätzlich umgesetzt werden müssen.

Der Baustein enthält keine organisatorischen Anforderungen zur Absicherung einer ICS-Komponente. Dafür müssen die Anforderungen des Bausteins IND.1 *Prozessleit- und Automatisierungstechnik* umgesetzt werden.

2. Gefährdungslage

Da IT-Grundschutz-Bausteine nicht auf individuelle Informationsverbünde eingehen können, werden zur Darstellung der Gefährdungslage typische Szenarien zugrunde gelegt. Die folgenden spezifischen Bedrohungen und Schwachstellen sind für den Baustein IND.2.1 *Allgemeine ICS-Komponente* von besonderer Bedeutung.

2.1. Unsichere Systemkonfiguration

Die Standardkonfiguration von ICS-Komponenten ist häufig darauf ausgelegt, dass die Komponenten korrekt funktionieren und sich leicht in Betrieb nehmen lassen. Sicherheitsmechanismen spielen dabei oft eine untergeordnete Rolle. So sind in der Standardeinstellung häufig alle Dienste, Protokolle und Anschlüsse eingeschaltet und bleiben aktiv, auch wenn sie nicht benutzt werden. Ebenso bleiben voreingestellte Berechtigungen häufig unverändert.

Es ist für Angreifende leicht, diese ICS-Komponenten zu übernehmen und zu manipulieren. Ebenso ist es möglich, dass bei einem Angriff die unsichere Systemkonfiguration ausgenutzt wird, um die ICS-Komponente als Ausgangspunkt für weitere Angriffe zu nutzen. In der Folge können institutionskritische Informationen abfließen oder auch der gesamte Betrieb der Institution beeinträchtigt werden.

2.2. Unzureichendes Benutzenden- und Berechtigungsmanagement

Einige ICS-Komponenten verfügen über ein eigenes Benutzenden- und Berechtigungsmanagement. Ist dieses unzureichend konzipiert, kann es passieren, dass Mitarbeitende gemeinsam Konten nutzen oder dass Berechtigungen von ausgeschiedenen Mitarbeitenden oder Dienstleistenden nicht gelöscht werden. Insgesamt können so unberechtigte Personen auf ICS-Komponenten zugreifen.

2.3. Unzureichende Protokollierung

Bei ICS-Komponenten beschränkt sich die Protokollierung häufig auf prozessrelevante Ereignisse. Für die Informationssicherheit relevante Daten werden oft nicht aufgezeichnet. Dadurch lassen sich Sicherheitsvorfälle nur schwer detektieren und hinterher nicht mehr rekonstruieren.

2.4. Manipulation und Sabotage einer ICS-Komponente

Die vielfältigen Schnittstellen von ICS-Komponenten führen zu einem erhöhten Manipulationsrisiko für IT-Systeme, die Software und übertragene Informationen. Je nach Motivation und Kenntnissen der Angreifenden kann sich das lokal, aber auch standortübergreifend auswirken. Zudem können Status- und Alarmmeldungen oder sonstige Messwerte unterdrückt oder verändert werden.

Manipulierte Messwerte können Fehlentscheidungen von ICS-Komponenten bzw. des Bedienpersonals nach sich ziehen. Manipulierte Systeme können dazu genutzt werden, um andere Systeme oder Standorte anzugreifen oder um eine laufende Manipulation zu vertuschen.

2.5. Einsatz unsicherer Protokolle

Die im Umfeld industrieller Steuerungsanlagen eingesetzten Protokolle bieten teilweise keine oder nur eingeschränkte Sicherheitsmechanismen. Technische Informationen wie Mess- und Steuerwerte werden häufig im Klartext und ohne Integritätssicherung oder Authentisierung übertragen. Dritte mit Zugang zum Übertragungsmedium können dann die Inhalte der Kommunikation auslesen und verändern oder Steuerbefehle einschleusen. So können Handlungen provoziert bzw. der Betrieb direkt beeinflusst werden. Ein Angriff auf Protokollebene ist auch dann möglich, wenn die ICS-Komponente ansonsten sicher konfiguriert ist und selbst keine Schwachstellen aufweist.

2.6. Denial-of-Service-(DoS)-Angriffe

Angreifende können den Betrieb von ICS-Komponenten durch DoS-Angriffe beeinträchtigen. Bei Prozessen, die unter Echtzeitbedingungen ablaufen, kann bereits eine kürzere Störung zu Informations- oder Kontrollverlusten führen.

2.7. Schadprogramme

Die Bedrohung durch Schadprogramme verschärft sich auch für industrielle Steuerungsanlagen immer mehr. Infektionsmöglichkeiten ergeben sich durch Schnittstellen zur Office-IT (vertikale Integration) und zur Außenwelt. Aber auch mobile Endgeräte wie Service-Notebooks oder Wechseldatenträger, die bei der Programmierung und Wartung von ICS-Komponenten eingesetzt werden, stellen eine Gefahr dar. Denn durch Letztere können Schadprogramme auch in isolierte Umgebungen eingebracht werden.

2.8. Ausspionieren von Informationen

ICS-Komponenten enthalten häufig detaillierte Informationen über den geregelten oder überwachten Prozess bzw. Vorgang. Auch aus sonstigen übertragenen Werten wie Mess- oder Steuerungsdaten lassen sich diese Informationen teilweise rekonstruieren. Gleiches gilt für Steuerungsprogramme oder -parameter.

Dritte könnten hier im Rahmen von Industriespionage an Geschäftsgeheimnisse gelangen, z. B. an Rezepte, Verfahren oder anderes geistiges Eigentum. Auch können sie Informationen über die Funktionsweise einer ICS-Komponente und ihre Sicherheitsmechanismen gewinnen, die sie für weitere Angriffe benutzen können.

2.9. Manipulierte Firmware

Bei ICS-Komponenten lässt sich neben dem Anwendungsprogramm auch das Betriebssystem (Firmware) verändern. Dadurch kann manipulierte Software in das System gelangen. Die internen Speicher könnten durch ein kompromittiertes Programmiergerät, über eine lokale Datenschnittstelle (z. B. USB) oder über eine andere bestehende Netzverbindung von Angreifenden verändert werden. Ebenso könnte ein Software-Update auf dem Weg vom herstellenden Unternehmen zum Betreibenden manipuliert worden sein. Schließlich könnte eine ICS-Komponente mit bereits kompromittierter Firmware beim Betreibenden eintreffen, etwa bei manipulierter Lieferkette (englisch *supply chain*) oder einem Einkauf aus unsicheren Quellen. Angreifende erhalten dadurch die Möglichkeit, Prozesse und Abläufe zu verändern bzw. zu verfälschen.

3. Anforderungen

Im Folgenden sind die spezifischen Anforderungen des Bausteins IND.2.1 *Allgemeine ICS-Komponente* aufgeführt. Der oder die Informationssicherheitsbeauftragte (ISB) ist dafür zuständig, dass alle Anforderungen gemäß dem festgelegten Sicherheitskonzept erfüllt und überprüft werden. Bei strategischen Entscheidungen ist der oder die ISB stets einzubeziehen.

Im IT-Grundschutz-Kompendium sind darüber hinaus weitere Rollen definiert. Sie sollten besetzt werden, insofern dies sinnvoll und angemessen ist.

Zuständigkeit	Rolle
Grundsätzlich zuständig	ICS-Informationssicherheitsbeauftragte
Weitere Zuständigkeiten	Mitarbeitende, Planende, Wartungspersonal, OT-Betrieb (Operational Technology, OT)

Genau eine Rolle sollte *Grundsätzlich zuständig* sein. Darüber hinaus kann es noch *Weitere Zuständigkeiten* geben. Falls eine dieser weiteren Rollen für die Erfüllung einer Anforderung vorrangig zuständig ist, dann wird diese Rolle hinter der Überschrift der Anforderung in eckigen Klammern aufgeführt. Die Verwendung des Singulars oder Plurals sagt nichts darüber aus, wie viele Personen diese Rollen ausfüllen sollen.

3.1. Basis-Anforderungen

Die folgenden Anforderungen MÜSSEN für diesen Baustein vorrangig erfüllt werden.

IND.2.1.A1 Einschränkung des Zugriffs auf Konfigurations- und Wartungsschnittstellen (B) [OT-Betrieb (Operational Technology, OT)]

Standardmäßig eingerichtete bzw. vom herstellenden Unternehmen gesetzte Passwörter MÜSSEN gewechselt werden (siehe ORP.4 *Identitäts- und Berechtigungsmanagement)*. Der Wechsel MUSS dokumentiert werden. Die Passwörter MÜSSEN sicher hinterlegt werden.

Es MUSS sichergestellt werden, dass nur berechtigte Mitarbeitende auf Konfigurations- und Wartungsschnittstellen von ICS-Komponenten zugreifen können. Die Konfiguration von ICS-Komponenten DARF NUR nach einer Freigabe durch die verantwortliche Person oder nach einer Authentisierung geändert werden.

IND.2.1.A2 Nutzung sicherer Übertragungs-Protokolle für die Konfiguration und Wartung (B) [Wartungspersonal, OT-Betrieb (Operational Technology, OT)]

Für die Konfiguration und Wartung von ICS-Komponenten MÜSSEN sichere Protokolle eingesetzt werden. Die Informationen MÜSSEN geschützt übertragen werden.

IND.2.1.A3 ENTFALLEN (B)

Diese Anforderung ist entfallen.

IND.2.1.A4 Deaktivierung oder Deinstallation nicht genutzter Dienste, Funktionen und Schnittstellen (B) [Wartungspersonal, OT-Betrieb (Operational Technology, OT)]

Alle nicht genutzten Dienste, Funktionen und Schnittstellen der ICS-Komponenten MÜSSEN deaktiviert oder deinstalliert werden.

IND.2.1.A5 ENTFALLEN (B)

Diese Anforderung ist entfallen.

IND.2.1.A6 Netzsegmentierung (B) [OT-Betrieb (Operational Technology, OT), Planende]

ICS-Komponenten MÜSSEN von der Office-IT getrennt werden. Hängen ICS-Komponenten von anderen Diensten im Netz ab, SOLLTE das ausreichend dokumentiert werden. ICS-Komponenten SOLLTEN so wenig wie möglich mit anderen ICS-Komponenten kommunizieren.

3.2. Standard-Anforderungen

Gemeinsam mit den Basis-Anforderungen entsprechen die folgenden Anforderungen dem Stand der Technik für diesen Baustein. Sie SOLLTEN grundsätzlich erfüllt werden.

IND.2.1.A7 Erstellung von Datensicherungen (S) [OT-Betrieb (Operational Technology, OT)]

Vor jeder Systemänderung an einer ICS-Komponente MÜSSEN Backups erstellt werden.

IND.2.1.A8 Schutz vor Schadsoftware (S) [OT-Betrieb (Operational Technology, OT)]

ICS-Komponenten SOLLTEN durch geeignete Mechanismen vor Schadprogrammen geschützt werden (siehe OPS.1.1.4 *Schutz vor Schadprogrammen*). Wird dafür ein Virenschutzprogramm benutzt, SOLLTEN das Programm und die Virensignaturen nach der Freigabe durch das herstellende Unternehmen immer auf dem aktuellen Stand sein.

Wenn die Ressourcen auf der ICS-Komponente nicht ausreichend sind oder die Echtzeitanforderung durch den Einsatz von Virenschutzprogrammen gefährdet werden könnte, SOLLTEN alternative Maßnahmen ergriffen werden, etwa die Abschottung der ICS-Komponente oder des Produktionsnetzes.

IND.2.1.A9 ENTFALLEN (S)

Diese Anforderung ist entfallen.

IND.2.1.A10 ENTFALLEN (S)

Diese Anforderung ist entfallen.

IND.2.1.A11 Wartung der ICS-Komponenten (S) [Mitarbeitende, OT-Betrieb (Operational Technology, OT), Wartungspersonal]

Bei der Wartung einer ICS-Komponente SOLLTEN immer die aktuellen und freigegebenen Sicherheitsupdates eingespielt werden. Updates für das Betriebssystem SOLLTEN erst nach Freigabe durch das herstellende Unternehmen einer ICS-Komponente installiert werden. Alternativ SOLLTE die Aktualisierung in einer Testumgebung erprobt werden, bevor diese in einer produktiven ICS-Komponente eingesetzt wird. Für kritische Sicherheitsupdates SOLLTE kurzfristig eine Wartung durchgeführt werden.

IND.2.1.A12 ENTFALLEN (S)

Diese Anforderung ist entfallen.